Volume: 6 Issue: IX Month of publication: September 2018

DOI:

A Review Paper on Smart Phone's Smart Security of Secret Questions

Krati Chauhan[1], Megha Singh[2]
[1, 2]CIIT, Indore

Abstract: Due to prevalence of smartphones the one issue which arises amongst the minds of most mobile user's is security. With our smartphone we carry lots of important data and if it is lost, trouble often ensues. Many online services offer two-factor authentication, which enhances security by requiring more than just your password to sign in. Currently we are using pin lock, alphanumeric lock, pattern lock, finger print lock and some other security techniques. Normal screen lock techniques are not completely secure, as anyone who peeps over your shoulder could see the secret word or the pin when you are entering it. You might hand your phone over to someone so they can make a call or look at a picture. Usually when you turn your back, that user could always look into your important data. Now a days few applications are made available while others are locked down. The increasingly use of smartphones has given us new opportunities to look at and perceive however the private knowledge collected by smartphone sensors and apps will facilitate produce personalized secret queries. In this paper we present an authentication system called "Authentication over Secret Questions" that creates a set of secret questions based on smartphone user's basic application usage, personal details and phone status. We will develop a prototype on Android smartphones and evaluate the security of secret questions by asking them to strangers who would answer the questions by guessing and without the help of online tools.

Keywords: Memorability, Prevalence, Two-factor authentication, Prototype, Secret Question

I. INTRODUCTION

These days we can find many cases of data theft by the intruders for making their own profit by using the hacked data. When talking about different types of attacks on personal data of users and precautions against them, there are many possible ways for both. Manually input passwords are the most commonly used security schemes in daily use applications. It has been scientifically proven that human brain configures a psychologically weak password, as they face problem remembering strong ones, which can easily be guessed by shoulder surfers.

Then came the pattern scheme in existence which is the most used security scheme till date for security in smartphone devices. Also the bio-metrics are being used on a large scale level such as banks, defense etc. but when it comes to personal use; it cannot be preferred due to its very high cost.

Apps related to networking services (i.e. chatting, social-networking, e-mailing, net-banking etc.) are more prone to attacks as they contain more important information. In this paper we propose an innovative idea related to android app security with the help of Secret questions. Secret questions have been widely used by many web applications as the secondary authentication method for reconfiguring the account password when the user login fails (For e.g. Email) [1].

When creating an online account, a user may be required to choose a secret question from a pre-determined list provided by the server, and set answers accordingly.

The user can reset his account password by providing the correct answers to the secret questions later. We had proposed a user authentication system with a bunch of secret questions created based on the data of users short-term smartphone usage. We have plan to evaluate the usability of the system, and find that proposed system is easier to use than those existing authentication system with secret questions based on users long term historic data.

Moreover, research findings in psychology show that one can easily memorize the details of his short-term activity, if this activity occurs multiple times during a short-term (e.g. Calling a friend many times), and/or this activity heavily involves his time and effort in a short time period (e.g., running exercise).

We had proposed a prototype named as "App Security through Secret Questions".

We will design an application in which user get questions which will he/she answer with the help of short term smartphone usage. A sample question with the category of question type is given below.

TABLE I
Font Sizes For Papers

No.	Questions	Category
1.	Was someone your most frequent contact last week?	Call
2.	What was the last call duration with your favorite contact?	Contact
3.	Which app did you install recently?	App usage
4.	Where is the birthmark on your body?	Personal
5.	Which place did you go on the weekend?	GPS
6.	Did you take photos in last three days?	Camera

II. RELATED WORK

In today's world, large number of smartphones running with Android operating system. As the smartphone use is increases, more amount of sensitive data are stored on their mobile devices [9]. One of the most common control mechanisms for authenticating users of computer based information systems is the use of passwords. However, despite the widespread use of passwords, only little attention has been given to the characteristics of their actual use. Sensitive data stored on smartphones creates many security issues like app security, protection of data on lost or stolen devices.

Smartphone sensors are used to get the data from short-term and long-term usage of smartphones. Through this data security questions are generated [1]. But when we used the smartphones to generate the security questions, we are not found that sensors are so reliable to get accurate data.

To easily recall, most secret questions are blank-fillings (eg., How many total number of apps installed in your smartphone?), and are created based on the long-term knowledge of a user's personal history that may not change over months/years. However, existing research has revealed that such blank-filling questions created upon the user's long-term history may lead to poor security and reliability [3][7].

R. Reeder and S. Schechter suggested the techniques to recover the forgotten password by Email-based authentication, Phone and other devices etc. for websites [2]. But the limitation for this system is, ooverreliance on weak security questions that don't match the authentication system's security level to the account's value, failure to keep secondary authentication data up to date

Zviran and Haga studied the security of secret questions for authentication in 1990 [3], which indicated that the answers of 33% questions can be guessed by the "significant others" who were mainly participants' spouses (77%) and close friends (17%). Another similar study was conducted by Podd et al, which revealed a higher rate of successful guessing (39.5%) [5]. A recent study showed that even an open question written by the user himself was still vulnerable to the guessing attacks launched by his acquaintance [5].

Swapnil Powar and Dr. B. B. Meshram in 2013 did the survey on Android Security Framework [10], in which they had concluded with the permission user grant while installing android app will produce harmful results.

Adarsh Singh,Ankit M.Dighraskar,Krutika R. Fulkar ,etl in 2016 presented a Implementation of Colour based Android Shuffling Pattern Lock [12]. Users found hard to remember the colon patterns.

III.PROPOSED FRAMEWORK

In this paper, we present an Authentication system based on Secret-Question, called "App Security through Secrete Questions", by making use of smartphone data and user's personal data.

With the data of users short-term smartphone usage we planned to create set of secrete questions with we had proposed a user authentication system. A minimum threshold will be set for the users and if the user satisfies the threshold he will be granted access to his personal application.

The proposed system will be divided into several independent modules:-

A. Personal Details

Here the user needs to enter the personal details that were only known by them. For example their star signs, their blood group, favourite colour, parents birth dates etc. These details are stored in database from which the security questions are raised. Since the personal details are converted as security questions it will be difficult for attacker to guess the answer. The data collected here are personalized data and will be hard to guess.

B. Monitor Phone

Next Module is monitoring our mobile phone data in order to increase the security. This process was separated into 3 phases, Application data, Phone status and Battery status. With users short-term smartphone usage a set of secrete questions are created. Most secret questions are blank-fillings and are created based on the long-term knowledge of a user's personal history. The frequently-changing secret questions will be difficult for attackers to guess the answers. We will use the local database to store the results generated after monitoring phone. We will store the result in encrypted format so that we can achieve more security.

C. User's Personal Application

Once the user correctly answers the questions more than the threshold limit then only he/she into his personal application which he has secured using our security application. In case the user login fails the application will be locked after a few attempts. If user not able to clear the threshold limits more than 3 attempts, in such cases we close the security app and send sms notification to emergency number which was registered at the time of registration.

The figure below depicts our proposed system.

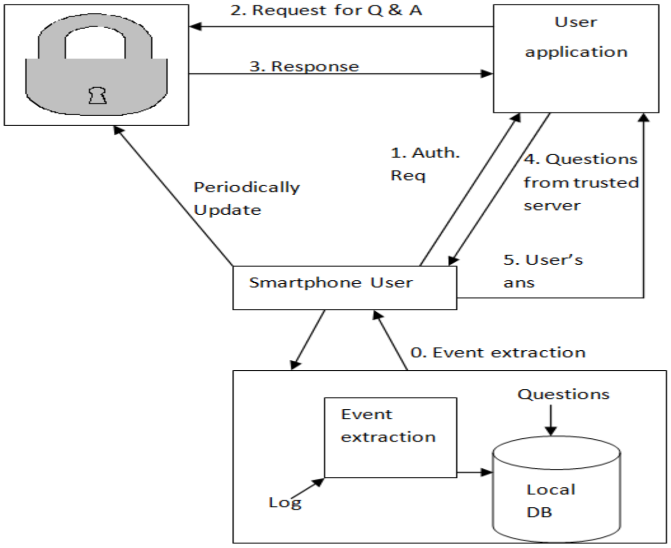

Fig.1. Architecture of Proposed System

IV. PROPOSED FRAMEWORK

First, we present a flow diagram for our system and then shows step by step how it works.

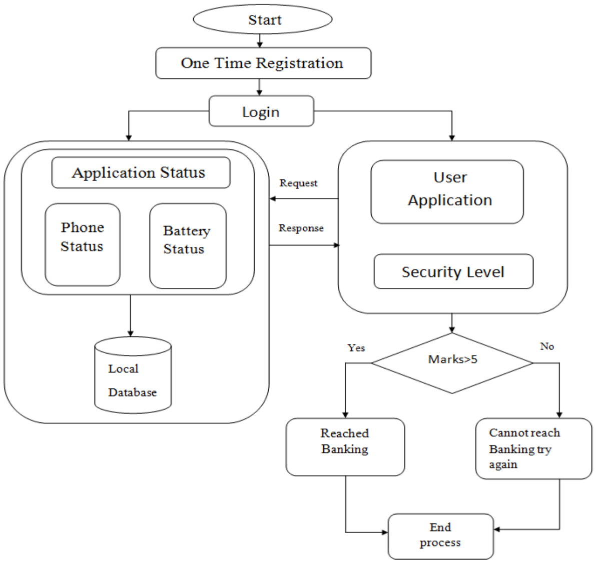

Fig.2. System Flow Diagram

1) *Step 1*: One time registration: In the first step we will create a 4-digit Personal Identification Number (PIN) for the smartphone user. We will also ask for the user's emergency phone number for sending alerts and security question for the recovery process.
2) *Step 2*: Using the generated PIN we will login into our security application.
3) *Step 3*: User needs to fill all personal details like name, date of birth of self and their parents, favorite color, sun sign, etc
4) *Step 4*: Our system will scan the phone status, application status and battery status. Based on this information a set of security questions will be generated and stored in the database.
5) *Step 5*: We will now click on the personal application upon which we have imposed our security application.
6) *Step* 6: Questions will get fired rapidly from the local database.
7) *Step* 7: If the user answers the questions correctly and satisfies the authentication criteria (For example: marks>5 ie. User has to answer minimum 5 questions out of the 7 questions) then user will be granted access to the personal application.
8) *Step 8*: If the user fails to answer the questions correctly more than 3 attempts then the application will stop working and an alert message will be send to emergency number

V. CONCLUSIONS

In this paper we have proposed a system which provides a clearer manifest as to the security and usability offered with challenging question authentication. In particular, with the help of personalize data with users short-term smartphone usage we will generate set of security questions, which are really hard to guess.

REFERENCES

[1] Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min Park, Xiaoming Li, Fan Ye, Wei Yan Understanding Smartphone Sensor and App Data for Enhancing the Security of Secrete Questions. IEEE Transactions on Mobile Computing, pp.99, 2016.

[2] R. Reeder and S. Schechter, When the password doesnt work: Secondary authentication for websites, S and P., IEEE, vol. 9, no. 2, pp. 4349, March 2011.

[3] M. Zviran and W. J. Haga, User authentication by cognitive passwords: an empirical assessment, in Information Technology, 1990.Next Decade in Information Technology, Proceedings of the 5th Jerusalem Conference on IEEE, 1990, pp. 137144.

[4] J. Podd, J. Bunnell, and R. Henderson, Cost-effective computer security: Cognitive and associative passwords, in Computer-Human Interaction, 1996. Proceedings., Sixth Australian Conference on. IEEE, 1996, pp. 304305.

[5] S. Schechter, A. B. Brush, and S. Egelman, Its no secret. measuring the security and reliability of authentication via secret questions, in S & P., IEEE, 2009, pp. 375390.

[6] S. Schechter, C. Herley, and M. Mitzenmacher, Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks, in USENIX Hot topics in security, 2010, pp. 18.

[7] D. A. Mike Just, Personal choice and challenge questions: A security and usability assessment, in SOUPS., 2009.

[8] A. Rabkin, Personal knowledge questions for fallback authentication: Security questions in the era of facebook, in SOUPS. ACM, 2008, pp. 1323.39.

[9] Sanjeev Srivastava, "Android Security Issues" https://www.cse.wustl.edu/~jain/cse571-14/ftp/android_security/index.html [online]

[10] Swapnil Powar, Dr. B. B. Meshram, , Survey on Android Security Framework, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 2" March -April 2013, pp.907-911.

[11] Arsalaan. F. Rashid, Mehreen Lateef, Balbir Kaur, O. P. Aggarwal, Sajad Hamid, Neeraj Gupta, Biometric Finger Print Identifcation Is It a Reliable Tool or Not?",J Indian Acad Forensic Med. April-June 2013, Vol. 35, No. 2.

[12] Adarsh Singh, Ankit M.Dighraskar,Krutika R. Fulkar ,etl, Implementation of Color based Android Shuffling Pattern Lock, Interbational Reasearch Jouranal og Engineering and Technology (IRJET), Feb-2016, Vol.03, pp,948-950.